[redacted]

L Number	Hits	Search Text	DB	Time stamp
1	176	(708/492).CCLS.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 12:43
2	6	((708/492).CCLS.) and @ad<19990120 and (inver$3).ti.	USPAT; US-PGPUB	2003/09/10 12:43
4	6	(((708/491-492) or (708/620)).CCLS.) and @ad<19990120 and (inver$3).ti.	USPAT; US-PGPUB	2003/09/10 12:43
7	2	((((708/491-492) or (708/620)).CCLS.) and @ad<19990120 and (inver$3).ti.) and ((shift adj register) "LSFB")	USPAT; US-PGPUB	2003/09/10 12:49
-	225	((@ad<19990120 and "finite field") and circuit) and arithmetic	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/04 15:59
-	47	(((@ad<19990120 and "finite field") and circuit) and arithmetic) and propagat$3	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/04 16:01
-	39	((((@ad<19990120 and "finite field") and circuit) and arithmetic) and propagat$3) and integer	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/04 16:01
-	4	((((@ad<19990120 and "finite field") and circuit) and arithmetic) and (carry near propagat$3)) and integer	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/04 16:02
-	6	(((@ad<19990120 and "finite field") and circuit) and arithmetic) and (carry near propagat$3)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/04 16:11
-	108	((380/28).CCLS.) and (galois "finite field")	USPAT; US-PGPUB	2003/09/04 16:13
-	28	"finite field" and ((without no) near carry)	USPAT; US-PGPUB	2003/09/04 16:55
-	5	"finite field" same ((without no) near carry)	USPAT; US-PGPUB	2003/09/05 09:17
-	3	"product-sum" and (finite adj field)	USPAT; US-PGPUB	2003/09/04 17:02
-	2	("product-sum" and (finite adj field)) and @ad<19990120	USPAT; US-PGPUB	2003/09/05 09:16
-	23	"elliptic" and "RSA" and coprocessor	USPAT; US-PGPUB	2003/09/05 09:57
-	702	((714/808) or (708/252,603,625,653,656)).CCLS.	USPAT; US-PGPUB	2003/09/09 09:40
-	635	(708/230,491,492,654,655).CCLS.	USPAT; US-PGPUB	2003/09/09 09:40
-	419	@ad<19990120 and iterat$4 and (modulo modulus modular) and (multipl$7) and $crypt$	USPAT; US-PGPUB	2003/09/09 10:42
-	154	@ad<19990120 and iterat$4 and (modulo modulus modular) and (divid$3 divis$3) and ("finite field" galois)	USPAT; US-PGPUB	2003/09/09 12:41
-	24	@ad<19990120 and ((modulo modulus modular remainder) same (divid$3 divis$3)) and (iterat$4 near subtract$3)	USPAT; US-PGPUB	2003/09/09 14:47
-	46	@ad<19990120 and (inverse same multipl$7 same divi$4) and ("finite field" galois) and (modulo)	USPAT; US-PGPUB	2003/09/09 15:02
-	2	@ad<19990120 and (inverse same multipl$7 same divi$4 same (instead rather)) and ("finite field" galois) and (modulo)	USPAT; US-PGPUB	2003/09/09 15:00
-	27	@ad<19990120 and (multipl$7 near divi$4 near inver$4)	USPAT; US-PGPUB	2003/09/09 16:00

-	39	(((@ad<19990120 and ((multipl$7 near inver$4) same divi$4)) not (@ad<19990120 and (multipl$7 near divi$4 near inver$4))) and @ad<19990120) and ("finite field" galois)	USPAT; US-PGPUB	2003/09/09 16:10
-	17	(multiplicative adj inverse).ti.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 16:29
-	4	("4473887" | "4567568" | "4574361" | "4800515").PN.	USPAT	2003/09/09 16:18
-	28	@ad<19990120 and (inver$3 and ("finite field" Galois)).ti.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 16:38
-	176	(708/492).CCLS.	USPAT; US-PGPUB	2003/09/09 17:20
-	2	(@ad<19990120 and (inverse same multipl$7 same divi$4 same (instead rather)) and ("finite field" galois) and (modulo)) and inverse	USPAT; US-PGPUB	2003/09/09 17:21
-	65	(@ad<19990120 and "multiplicative inverse") and (Galois "finite field")	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 08:41
-	48	((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 08:41
-	46	(((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and bit	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 08:41
-	25	((((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and bit) and significant	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 09:22
-	25	(((((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and bit) and significant) and inver$4	USPAT; US-PGPUB	2003/09/10 09:22
-	26	(((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and significant	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 09:22
-	25	((((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and significant) and inver$4	USPAT; US-PGPUB	2003/09/10 11:00
-	66	(@ad<19990120 and inver$4 and (linear adj feedback adj shift adj register)) and galois	USPAT; US-PGPUB	2003/09/10 11:07
-	59	((@ad<19990120 and inver$4 and (linear adj feedback adj shift adj register)) and galois) not (((((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and significant) and inver$4)	USPAT; US-PGPUB	2003/09/10 11:09
-	4	(((@ad<19990120 and inver$4 and (linear adj feedback adj shift adj register)) and galois) not (((((@ad<19990120 and "multiplicative inverse") and (Galois "finite field")) and shift$3) and significant) and inver$4)) and (multiplicative adj inverse)	USPAT; US-PGPUB	2003/09/10 13:55

Modular arithmetic and finite field theory: A tutorial

Full text Pdf (569 KB)

Source **Symposium on Symbolic and Algebraic Manipulation** archive
Proceedings of the second ACM symposium on Symbolic and algebraic manipulation table of contents
Los Angeles, California, United States
Pages: 188 - 194
Year of Publication: 1971

Author E. Horowitz

Sponsors SIGNUM: ACM Special Interest Group on Numerical Mathematics
SIGART: ACM Special Interest Group on Artificial Intelligence
SIAM : Society for Industrial and Applied Mathematics
SIGPLAN: ACM Special Interest Group on Programming Languages
SIGSAM: ACM Special Interest Group on Symbolic and Algebraic Manipulation

ABSTRACT

The paradigm of algorithm analysis has achieved major pre-eminence in the field of symbolic and algebraic manipulation in the last few years. A major factor in its success has been the use of modular arithmetic. Application of this technique has proved effective in reducing computing times for algorithms covering a wide variety of symbolic mathematical problems. This paper is intended to review the basic theory underlying modular arithmetic. In addition, attention will be paid to certain practical problems which arise in the construction of a modular arithmetic system. A second area of importance in symbol manipulation is the theory of finite fields. A recent algorithm for polynomial factorization over a finite field has led to faster algorithms for factorization over the field of rationals. Moreover, the work in modular arithmetic often consists of manipulating elements in a finite field. Hence, this paper will outline some of the major theorems for finite fields, hoping to provide a basis from which an easier grasp of these new algorithms can be made.

REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 Berlekamp, E.R, Algebraic Coding Theory, McGraw-Hill Book Co., New York, 1968, Chapters 2,4, and 6.

2 Berlekamp,E.R, "Factoring polynomials over large finite fields," Mathematics of Computation, July, 1970.

3 Borosh, I. and A.S. Fraenkel, "Exact solution of linear equations with rational coefficients by congruence techniques," Mathematics of Computation, Vol. 20, No. 93 (January 1966), pp. 107-112.

4 W. S. Brown, On Euclid's algorithm and the computation of polynomial greatest common divisors, Proceedings of the second ACM symposium on Symbolic and algebraic manipulation, p.195-211, March 23-25, 1971, Los Angeles, California, United States

5 Collins, G.E., "Computing multiplicative inverses in GF(p)," Mathematics of Computation, Vol. 23, No. 105 (January 1969, pp. 197-200.

6 Collins, G.E. "Computing time analysis of some arithmetic and algebraic algorithms," Proceedings of the IBM 1968 Summer Institute on Symbolic Mathematics by Computer, IBM Boston Programming Center, Cambridge, Mass, June 1969, pp. 195-232.

7 George E. Collins, The calculation of multivariate polynomial resultants, Proceedings of the second ACM symposium on Symbolic and algebraic manipulation, p.212-222, March 23-25, 1971, Los Angeles, California, United States

8 Collins, G.E., and E Horowitz, et al., "The SAC-1 modular arithmetic system," Computing Center and Computer Sciences Department, University of Wisconsin, Technical Reference No. 10, June 1969.

9 Collins, G.E. and E Horowitz, "The SAC-1 partial fraction decomposition and rational function integration system." Computing Center and Computer Sciences Department, University of Wisconsin, Technical Reference No. 80, February 1970.

10 Dickson, E.L. Introduction to the Theory of Numbers, Dover Publications, Inc, New York, 1929.

11 Feldman, H.A., "Some symbolic computations in finite fields", Proceedings of the IBM Summer 1968 Institute on Symbolic Mathematics by Computer, IBM Boston Programming Center, Cambridge, Mass, June 1969, pp. 79-96.

12 Aviezri S. Fraenkel, The Use of Index Calculus and Mersenne Primes for the Design of a High-Speed Digital Multiplier, Journal of the ACM (JACM), v.8 n.1, p.87-96, Jan. 1961

13 Garner, H.L. "The residue number system" IRE Transactions, EC-8 (1956), pp 140-147.

14 Ellis Horowitz, Algorithms for partial fraction decomposition and rational function integration, Proceedings of the second ACM symposium on Symbolic and algebraic manipulation, p.441-457, March 23-25, 1971, Los Angeles, California, United States

15 Horowitz, E. Algorithms for Symbolic Integration of Rational Functions, PhD Dissertation, University of Wisconsin, Madison, Wisconsin, November 1969.

16 Howell, J. A. and R. T. Gregory, "An algorithm for solving linear algebraic equations using residue arithmetic I," BIT, Vol. 9 (1969) ,pp 200-224.

17 Howell, J. A. and R. T. Gregory, "Solving linear equations using residue arithmetic-Algorithm II", TNN-95, Computation Center University of Texas at Austin, September 1969.

18 Donald E. Knuth, The art of computer programming, volume 1 (3rd ed.): fundamental algorithms, Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, 1997

19 Donald E. Knuth, The art of computer programming, volume 2 (3rd ed.): seminumerical algorithms, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 1997

20 Takahasi, H., and Y. Ishibashi, "A new method for exact calculation by a digital computer," Information Processing in Japan, Vol. 1 (1961), pp. 28-42.

21 Van der Waerden, B.L., Modern Algebra, translated by F. Blum, Vol. 1, New York, Ungar Publishing, 1949.

22 Szabo, N.S. and R.I. Tanaka, Residue Arithmetic and It's application to Computer Technology, McGraw-Hill, New York, 1967.

CITINGS 2

Ellis Horowitz, Algorithms for rational function arithmetic operations, Proceedings of the fourth annual ACM sumposium on Theory of computing, p.108-118, May 01-03, 1972, Denver, Colorado, United States

B. F. Caviness , G. E. Collins, Symbolic mathematical computation in a Ph.D. computer science program, Papers of the second ACM SIGCSE symposium on Education in computer science, p.19-23, March 01-01, 1972

INDEX TERMS

Primary Classification:

F. Theory of Computation

- **F.2** ANALYSIS OF ALGORITHMS AND PROBLEM COMPLEXITY
  - **F.2.1** Numerical Algorithms and Problems
    - **Subjects:** Computations in finite fields

Additional Classification:

F. Theory of Computation

- **F.2** ANALYSIS OF ALGORITHMS AND PROBLEM COMPLEXITY
  - **F.2.1** Numerical Algorithms and Problems
    - **Subjects:** Number-theoretic computations (e.g., factoring, primality testing)

I. Computing Methodologies

- **I.1** SYMBOLIC AND ALGEBRAIC MANIPULATION
  - **I.1.0** General

General Terms:

Algorithms, Theory

Keywords:

Exact multiplication, Finite fields, Modular arithmetic, Symbol manipulation;

Collaborative Colleagues of:

E. Horowitz:

Y. Bao

M. C. Horowitz
H. L. Morgan
J. B. Munson
S. Sahni
A. C. Shaw

Peer to Peer - Readers of this Article have also read:

- Data structures for quadtree approximation and compression
  Communications of the ACM 28, 9
  Hanan Samet

- The state of the art in automating usability evaluation of user interfaces
  ACM Computing Surveys (CSUR) 33, 4

- A lifecycle process for the effective reuse of commercial off-the-shelf (COTS) software
  Proceedings of the 1999 symposium on Software reusability
  Christine L. Braun

- A catalog of techniques for resolving packaging mismatch
  Proceedings of the 1999 symposium on Software reusability
  Robert DeLine

- Using adapters to reduce interaction complexity in reusable component-based software development
  Proceedings of the 1999 symposium on Software reusability
  David Rine , Nader Nada , Khaled Jaber